

*Sub A2* > **WHAT IS CLAIMED IS:**

1. A computer-readable medium having computer-executable instructions for performing a process, the process comprising:  
5 monitoring access by a host server of digital tracking components residing on a remote client during digital communication between the remote client and the host server; and

providing an alert to the remote client when the host server requests one or more of the digital tracking components that contains information that is not associated with the host server.

10

2. The computer-readable medium for performing a process of claim 1, wherein the information is information about the remote client that is associated with other host servers.

15

3. The computer-readable medium for performing a process of claim 1, wherein the information that is not associated with the host server making the request contains confidential information.

20

4. The computer-readable medium for performing a process of claim 1, wherein the alert is a visual alert.

5. The computer-readable medium for performing a process of claim 1, wherein the alert is an audible alert.

25

6. The computer-readable medium for performing a process of claim 1, wherein the remote client communicates with the host server via a networked connection.

30

7. The computer-readable medium for performing a process of claim 6, wherein the networked connection is a World Wide Web Internet connection.

8. The computer-readable medium for performing a process of claim  
7, wherein the method operates within a World Wide Web browser.

5

9. The computer-readable medium for performing a process of claim  
8, wherein the digital tracking component is a cookie that is used by the World  
Wide Web browser.

10

10. The computer-readable medium for performing a process of claim  
1, further comprising displaying in symbolic format the digital tracking  
components that the remote client has residing in a memory location.

15

11. In a computer system having a connection between a remote  
client and a host server, a method of protecting the remote client from  
digital intrusions, the method comprising:

monitoring access by host servers of digital tracking components  
of the remote client; and

20

providing an alert to the remote client when a request of a  
particular digital tracking component by a particular host server is made if the  
particular host server is not associated with the requested digital tracking  
component.

25

12. The method of claim 11, wherein the remote client includes a  
graphical user interface including a display and a user interface selection  
device for providing the alerts.

13. The method of claim 11, wherein the alerts are provided as audible alerts.

14. The method of claim 12, wherein the alerts are provided by displaying the alert via the user interface to the remote client to indicate a request of a particular digital tracking component by a particular host server and whether the particular host server is associated with the requested digital tracking component.

10 15. The method of claim 14, wherein the connection between the remote client and the host server is a World Wide Web Internet connection.

15 16. A computer security system for preventing host servers from taking inappropriate self-contained packets of information residing on a remote client, the system comprising:

a monitor module that monitors requests by the host servers of the self-contained packets of information residing on a remote client during digital communication between the remote client and the host server; and

20 25 a notify module that provides a notification to the remote client when a particular host server requests one or more of the self-contained packets of information that contains information that is not associated with the particular host server.

17. The computer security system of claim 16, wherein the notification is a visual alert.

18. The computer security system of claim 16, wherein the alert is an audible alert.

19. The computer security system of claim 16, wherein the monitor and notify modules operate within a World Wide Web browser and the self-contained packets of information are cookies.

5

20. The computer security system of claim 19, wherein the notify module displays in symbolic format the cookies that the remote client has residing in a memory location.

10

21. A method of transacting data between a first and a second computer, comprising:

monitoring data requests from the first computer by the second computer;

determining whether the second computer should have access to the data requested; and

preventing the second computer from accessing the data if it is determined that the second computer should not have access to the data.

15

22. The method of claim 21, wherein the transaction of data occurs over the Internet.

20

23. The method of claim 22, wherein the data is a digital tracking component.

25

24. The method of claim 23, wherein the transaction of data occurs within a World Wide Web browser environment and the digital tracking component is a cookie.

DOCKET 2000-0323-US1

25. A computer-readable medium having computer-executable instructions for performing a process for transacting data between a first and a second computer, the process comprising:

5 monitoring data requests from the first computer by the second computer;

determining whether the second computer should have access to the data requested; and

10 preventing the second computer from accessing the data if it is determined that the second computer should not have access to the data.

10 26. The computer-readable medium for performing a process of claim 25, wherein the transaction of data occurs over the Internet.

15 27. The computer-readable medium for performing a process of claim 26, wherein the data is a digital tracking component.

20 28. The computer-readable medium for performing a process of claim 27, wherein the transaction of data occurs within a World Wide Web browser environment and the digital tracking component is a cookie.

20 29. A computer security system for preventing inappropriate transaction of data between a first and a second computer, the system comprising:

25 a monitor module that monitors data requests from the first computer by the second computer;

an access module that determines whether the second computer should have access to the data requested; and

30 a prevent module that prevents the second computer from accessing the data if it is determined that the second computer should not have access to the data.

30. The computer security system of claim 29, wherein the transaction of data occurs over the Internet.

5           31. The computer security system of claim 30, wherein the data is a  
digital tracking component.

32. The computer security system of claim 31, wherein the transaction  
of data occurs within a World Wide Web browser environment and the digital  
tracking component is a cookie.